



Frequently Asked Questions

Version 10-21-2016

Copyright © 2014-2016 Aviatrix Systems, Inc. All rights reserved.

Aviatrix Cloud Gateway

What can it do for me?

Aviatrix Cloud Gateway provides an end to end secure network solution for AWS, Azure and Google GCloud. The solution includes an enterprise OpenVPN access to VPC/VNet, encrypted routing among VPC/VNets and monitoring and logging of link status and latency. The solution enables you to build a secure private network spanning one or more public clouds where a user access any instance/VM with a private IP address directly. No more bastion stations and jump hosts, the solution gives user the seamless experience that they enjoy when using the on-prem network.

In addition, Aviatrix Cloud Gateway supports encryption over AWS Direct Connect and Azure Express Route.

Architecturally, Aviatrix solution is a centrally managed, loosely coupled and globally deployed platform built for the cloud from the ground up.

Key benefits?

- Scalable and highly available user VPN solution.
 - Integrated with cloud provider native ELB, the solution scales out to unlimited number of users and bandwidth.
 - Supports multi factor authentication: DUO, LDAP and OKTA.
 - User profile defined dynamic security access rules that allow administrator to determine access privilege of any given user to any resources at the network perimeter.
 - Supports Geo VPN for a global VPN solution deployment where a VPN user automatically connects to a nearest VPC.
 - Supports wide range of clients: Windows, OSX, Linux, Android, iOS, and Chromebook.
 - Supports event logging with SumoLogic, Logstash, Splunk and remote syslog server.
 - Supports Split tunnel and full tunnel mode.
 - No extra hop to other VPC/VNets.

- multi VPC, multi region and multi cloud (AWS, Azure and GCloud) encrypted peering enables you to build a full mesh secure network in the cloud with a single click.
- Policy based stateful firewall at the VPC level for both access and deny to apps.
- Environment Stamping solution for repeatable enterprise SaaS deployment.
 - Create identical VPC environments with one click for each customer.
 - Uniquely mapping and addressing instances for CloudOps and developers access.
 - Integrate AWS Route 53 DNS name service for each accessing.
- Secure connection to remote branch sites and interoperability with legacy router/firewall device.
- Encryption over AWS Direct Connect and Azure Express Route.

How do I launch the product?

The product consists of two components, the controller and one or more gateways. The gateway is launched from the controller.

The controller provides a central console for all provisioning, monitoring and upgrades of the services.

The controller is available in AWS and Azure marketplace. It is also available as a GCloud community image. For marketplace launch, search for “Aviatrix” in marketplace.

The controller should have an EIP (best practice) address and inbound TCP port 443 open for it to work.

How do I access the controller?

Once you have launched the instance, you access the Controller instance via a web browser.

`https://public_IP_address_of_the_controller_instance`

Login with username “admin”. The first time password is the private IP address of the controller instance. You are required to change the password at your first login.

How do I secure the controller?

Only TCP port 443 needs to be opened for inbound traffic to the controller. If you wish to reduce the scope of source addresses by specifying custom IP address, you must include all gateway public IP addresses, in addition to your own public IP address. This is because gateways launched from the controller use its public IP address to communicate back to controller.

Is Aviatrix Cloud Gateway a SaaS offer?

No. Aviatrix Cloud Gateway is a software product that is deployed in your own network perimeter.

Onboarding

Where do I start?

The first time when you login, complete Onboarding process. It takes a few steps.

If you have a BYOL license or use a community image, you need to have a customer ID provided by Aviatrix to be able to use the product. Contact support@aviatrix.com if you do not have a customer ID.

What is an Aviatrix Cloud Account?

An Aviatrix Cloud Account is specific and unique on the controller. It contains cloud credentials, for example, your AWS IAM Access Key ID and Secret Key. The controller uses these credential to launch Aviatrix gateways by using cloud APIs.

An Aviatrix Cloud Account can correspond to multiple cloud account. For example, it can contain credentials for an AWS IAM account, Azure account and GCloud account.

How do I upgrade software?

Click Settings -> Upgrade. This upgrades to the latest release of the controller software.

When a new release becomes available, an alert message appears on Dashboard.

Is there a reference design example?

Check out multiple Reference Designs under Help menu.

What is the support model?

For support, send email to support@aviatrix.com. To request a feature, click Make a wish button at the bottom of each page.

Scale Out VPN Solutions

How do I launch a VPN gateway?

Click Gateways -> Create Gateway -> Create

The controller launches an Aviatrix gateway instance in AWS/Azure/GCloud. The gateway instance must be launched from a public subnet. You need to give it a name (The name is presented as a Gateway Name field), this name becomes part of the instance name with a prefix CloudOps.

In the Create page, select VPN Access to enable OpenVPN server capability. There is a default VPN CIDR "192.168.43.0/24". But you can change it, make sure the CIDR is outside the existing and future VPC CIDR range. This VPN CIDR is where VPN server assign virtual IP address to each user when she connects.

You can select Save Template to save the gateway template. When you come to the page the next time, most of the fields are pre populated. You may change any of the fields.

How do I scale out VPN solution?

You can launch multiple VPN gateways in the same VPC at the Create Gateway time.

While launching a gateway, select yes for "Enable AWS ELB". This will automatically create an AWS ELB (for the first gateway) and register the gateway with the newly created load balancer. VPN traffic will be load balanced across these multiple gateways.

It is required to have consistent gateway configuration when ELB is enabled. For example, authentication methods, tunnel modes and PBR configurations should be identical.

How do I setup Okta authentication for VPN?

Follow the link: [How to setup Okta for Aviatrix VPN gateway](#)

How do I enable Geo VPN?

If you have global workforce that needs to access the cloud, Geo VPN offers a superior solution. Geo VPN enables a VPN user to connect to a nearest VPC that hosts Aviatrix VPN gateway.

To enable Geo VPN, go to VPC/VNet -> VPN Access -> Geo VPN.

How do I add a VPN user?

After at least one gateway is created, you can add VPN users.

Click VPCs -> VPN Access -> Users -> Add to add a VPN user.

When a user is added, an email is sent to the user with instructions on how to download client software and connect to VPN server.

If you like to assign user profile based policies, you need to create profiles first, see the next section.

What user devices are VPN client software supported?

Windows, MAC, Linux, Chromebook, Android and iOS devices are supported.

Is NAT capability supported on the gateway?

Yes, you can enable NAT function at gateway launch time. When enabled, instances on the private subnet can access Internet directly.

If full tunnel mode is selected, you may want to enable NAT to allow instances in the VPC to have direct Internet access.

Is full tunnel mode supported on the gateway?

Yes, both split tunnel and full tunnel modes are supported. You can specify the mode at the gateway launch time.

Full tunnel means all user traffic is carried through the VPN tunnel to the gateway, including Internet bound traffic.

Split tunnel means only traffic destined to the VPC and any additional network range is carried through the VPN tunnel to the gateway. Any Internet bound traffic does not go through the tunnel.

Can the maximum number of simultaneous connections to VPN gateway be configured?

Yes, you can set the maximum number of connections at the gateway launch time.

User Profile Based Security Policies

What is user profile based security policy?

In VPN access, a user is dynamically assigned a virtual IP address when connected to a gateway. It is highly desirable to define resource access policies based on the users. For example, you may want to have a policy for all employees, a different policy for partners and a still different policy for contractors. You may even give different policies to different departments and business groups.

The profile based security policy lets you define security rules to a target address, protocol and ports. The default rule for a profile can be configured as deny all or allow all during profile creation. This capability allows flexible firewall rules based on the users, instead of a source IP address.

How do I setup profile based security policies?

When a user connects to a VPC, the security policies associated with the profile that the user is assigned to are applied to the VPN gateway instance that user logs in. This effectively blocks traffic from entering the network.

Click VPCs -> VPN Access -> Profiles to create profiles, then click Edit Policies to add rules. You can add multiple of them, then click on Save.

How do I assign a user to a profile?

When you create a VPN user at VPCs -> VPN Access -> Users -> Add, you can select profile option to assign the user to a specific profile.

What if I want to change profile policies?

You can change profile policies any time. However, the users who are currently active in session will not receive the new policy. The user need to disconnect and reconnect to VPN for the new policy to take effect.

How do I change a user's profile programmatically?

The controller provides a REST API which can be invoked to change a user's profile. Refer to API document under Help menu.

During this operation, the user's existing VPN session will be terminated. The new profile policy will take effect when he or she logs in again.

The use case for this feature is to allow administrator to quarantine a VPN user for security reasons.

User Authentication

Is DUO multi-factor authentication supported?

Yes. If your enterprise has a DUO account with multi-factor authentication, it can be integrated into the VPN solution. From Gateways tab, click Create. At two-step authentication drop down menu, select DUO, then enter your company Integration Key, Secret Key and API hostname.

To obtain Integration Key, Secret key and API hostname, login to DUO website as an admin, www.duo.com, click on the left panel Applications, click Protect an Application below. Scroll down the application list and select OpenVPN (click Protect this Application), the next screen should reveal the credentials you need to configure on the Aviatrix controller.

Currently advanced feature such as Trusted Device and Trusted Networks are not supported. Send us a request if you like to integrate these features.

How do I configure LDAP authentication?

LDAP configuration is part of the Gateway creation when VPN Access is enabled. Enter the necessary parameters and click Enable button to enable LDAP authentication for VPN clients. If your LDAP server is configured to demand client certificates for incoming TLS connections, upload a client certificate in PEM format (This certificate should contain a public and private key pair).

Can I combine LDAP and DUO authentication?

Yes. With both LDAP and DUO authentication methods enabled on a gateway, when launching the VPN client, a remote user will have to enter his or her LDAP user credentials and then approve the authentication request received on a registered mobile device to login to VPN.

Is OKTA supported?

Yes. OKTA with MFA is also supported. Follow the [instructions](#)

Policy Based Routing

How does Policy Based Routing (PBR) work?

When PBR is enabled at gateway launch time, all VPN user traffic arrives at the gateway will be forwarded to a specified IP address defined as PBR default gateway. User must specify the PBR Subnet which in AWS must be in the same availability zone as Ethernet 0 interface of the gateway.

When PBR feature is combined with encrypted peering capability, VPN user should be able to access any instances in the peered VPC/VNets. This helps build an end to end cloud networking environment. For details, check out our [reference design](#).

Another use case for Policy Based Routing is if you like to route all Internet bound traffic back to your own firewall device on Prem, or log all user VPN traffic to a specific logging device, PBR lets you accomplish that.

Logging and Monitoring

How do I forward syslog events to my Logstash server?

Click on Settings-> Logging ->LogStash logging and input the required parameters to enable forwarding of controller syslog events and all gateways syslog and auth log to a Logstash server.

SUMO Logic, Splunk and rSyslog are also supported.

What are the monitoring capabilities?

Active VPN users are displayed on the Dashboard. Click on any username, the user VPN connectivity history is displayed.

You can also disconnect a user from the dashboard.

Is there an Operator account?

Yes, you can create an operator account. This operator account can only view dashboard and disconnect an active user from the dashboard.

To create an Operator account, go to Settings -> Accounts -> Add. At the account name, type in "Operator" and give it a password and email notification address. You do not need to enter AWS credentials.

Encrypted peering

What can Aviatrix encrypted peering do?

Aviatrix encrypted peering builds an encrypted tunnel between two VPC/VNet with a single click. The VPC and/or VNet can be across region and across cloud. The solution enables you to build a full mesh encrypted network. You can enable stateful firewalls on each VPC/VNet to add additional security measures.

How do I configure encrypted peering?

Step 1: At Gateway menu, create a gateway in one existing VPC/VNet. VPN access may be disabled.

Step 2: Repeat Step 1 with a different VPC ID or VNet Name.

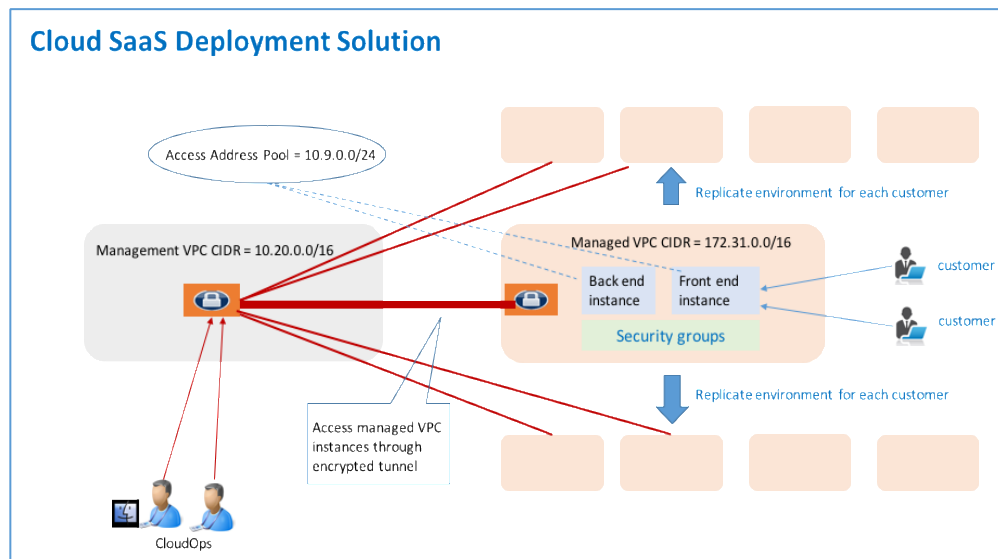
Step 3: At VPC/VNet Menu -> Encrypted Peering -> Add. Select the two gateway names and click Save.

Environment Stamping Networking

What does Environment Stamping networking feature do?

Environment Stamping (envStamping) takes advantage of the unique nature of Virtual Private Cloud (VPC) and offers a deployment architecture that is secure and scalable.

envStamping provides a deployment solution where you can create identical environments such as identical VPC CIDRs and access instances in the VPC seamlessly and securely via encrypted tunnel, as shown in the picture below:



In the above picture, each managed VPC shares identical CIDRs, instances private IP addresses and security groups. CloudOps and developers access VPC instances by connecting to the gateway in the management VPC via Aviatrix VPN capability.

Who should be deploying this model?

This deployment model allows for infinite scale of deployment, it is suitable for SaaS providers, development and testing. With this model, SaaS provider can offer secure and single tenant to its enterprise customers, while being able to access instances for maintenance and support.

For example, a SaaS provider can offer an enterprise customer its own AWS account and VPC environment. Customer data is completely isolated from others. Only authorized personal can access customer instances for maintenance and troubleshooting.

What is the workflow to enable this feature?

Refer to this [link](#) for workflow steps.

Administration

Can there be multiple admins?

Yes. Username “admin” is the default admin user. But you can create multiple users with admin privilege. Check out a reference design under Help to learn more about setting up multiple admin users.

Is there 2FA support to log in to the console?

Yes. In addition to password login, DUO authentication is supported.